

18 - 3522 JMC

18 - 3523 JMC

IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF) Case No.
HP DESKTOP COMPUTER S/N 3CR61007ML (A1);)
DELL ALL-IN-ONE COMPUTER S/N HWRN872 (A2);)
IPHONE IMEI# 356572083172807 (A3);) <u>UNDER SEAL</u>
IPHONE S/N 354854092408816 (A4);)
WINDOWS SURFACE PRO 8 S/N 012683151853 (A5))
MACBOOK PRO S/N C02WT03ZHV2M (A6))

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, George J. Wahl, , being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— six electronic devices A1 - A6—which are currently in law enforcement possession, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent (“SA”) of the Federal Housing Finance Agency – Office of the Inspector General (“FHFA-OIG”). I have been a SA with the FHFA-OIG since April 2013. I am assigned to the Northeast Region of the FHFA-OIG, which conducts investigations relating to, among other things, bank and mortgage fraud, and am currently detailed to the Federal Bureau of Investigation, Baltimore Field Office, Complex Financial Crimes Squad as a Task Force Officer.

3. Prior to my employment with the FHFA-OIG, I was a Special Agent with the United States Secret Service (“USSS”) and was employed by that agency beginning in 2002. During that time, I received formal training in the investigation of financial crimes, including bank fraud, counterfeiting of United States currency, and identity theft. I have received training at the Federal

On Hold
18 - 3522 JMC

18 - 3523 JMC

Law Enforcement Training Center in Glynco, Georgia and the USSS James J. Rowley Training Center in Beltsville, Maryland. I have investigated or assisted in the investigation of numerous cases involving fraudulent activity, including mortgage fraud, bank fraud, access device fraud, and identity theft. I have been a sworn law enforcement officer since 2003 and was assigned to the USSS Washington Field Office, Metropolitan Area Fraud Task Force, and investigated violations of federal laws, including violations of 18 U.S.C. §§ 1014 (Loan Application Fraud), 1341 (Mail Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), and 1957 (Money Laundering). I have received extensive specialized training in these fields.

4. Through my training and experience, I have become familiar with the methods and techniques used by criminals to commit economic crimes, such as wire fraud, bank fraud, and how those criminals conceal and store information derived from such criminal activity.

5. This affidavit is intended to show merely there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1349 (Conspiracy to Commit Wire Fraud), 1343 (Wire Fraud), 1028A (Identity Theft), 1956(h) (Money Laundering Conspiracy), and 1957 (Financial Transactions Over \$10,000 in Criminally Derived Property) have been committed by **JAY BRIAN LEDFORD ("LEDFORD")**, **KEVIN B. MERRILL ("MERRILL")** and **CAMERON R. JEZIERSKI ("JEZIERSKI")** and that there is probable cause to search the electronic devices A1 - A6 named above (the "Target Devices") for evidence of these crimes as further described in Attachment B.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. The Target Devices to be searched are:

18 - 3522 JMC

18 - 3523 JMC

- HP DESKTOP COMPUTER S/N 3CR61007ML (A1)
- DELL ALL-IN-ONE COMPUTER S/N HWRN872 (A2)
- IPHONE IMEI# 356572083172807 (A3)
- IPHONE S/N 354854092408816 (A4)
- WINDOWS SURFACE PRO 8 S/N 012683151853 (A5)
- MACBOOK PRO S/N C02WT03ZHV2M (A6)

The Target Devices are currently located in the Evidence Control Center, FBI Baltimore Field Office, 2600 Lord Baltimore Drive, Baltimore, Maryland.

8. The applied for warrant would authorize the forensic examination of the Target Devices as particularly described in Attachment B for the purpose of identifying electronically stored data which is evidence and instrumentalities of the crimes set forth in ¶5.

STATEMENT OF PROBABLE CAUSE

9. On September 11, 2018, MERRILL, LEDFORD, and JEZIERSKI were indicted in the District of Maryland on charges of 18 U.S.C. §§ 1349 (Conspiracy to Commit Wire Fraud), 1343 (Wire Fraud), 1028A (Identity Theft), 1956(h) (Money Laundering Conspiracy), Financial Transactions Over \$10,000 in Criminally Derived Property. Criminal No. RDB-18-0465, ECF 1.

10. On September 18, 2018, MERRILL was arrested at his home in Towson, MD and LEDFORD and JEZIERSKI were arrested in Las Vegas, NV at the Mirage Hotel and Casino, all pursuant to federal arrest warrants. During the arrests of both LEDFORD and JEZIERSKI, the Devices A1 to A6 were located in their respective hotel villa (LEDFORD) and hotel room (JEZIERSKI). Devices A4 to A6 were found in JEZIERSKI's hotel room, were seized incident to arrest by arresting agents, and placed into evidence. Device A3 was seized from LEDFORD incident to his arrest. Agents did not have a search warrant for LEDFORD's villa and thus Devices A1 and A2 were not seized at the time of LEDFORD's arrest. A1 and A2 were taken by Mirage Hotel and Casino security staff as abandoned property after LEDFORD was taken into custody.

18 - 3522 JMC

18 - 3523 JMC

At the time of his arrest, LEDFORD was living in Las Vegas, Nevada, but the business entities he controlled were in the Dallas, Texas area, which is also where JEZIERSKI lived. MERRILL lived in Maryland, but frequently traveled to Texas and other locations to meet with investors and potential investors.

11. At the time of LEDFORD's arrest, Target Device A1, a desktop computer, was found in his hotel room at the Mirage Hotel and Casino. Your affiant knows, based on his training and experience, that desktop computers are large devices that often require multiple cables and peripheral devices, and are generally not intended to be mobile in nature. Your Affiant has learned that LEDFORD had stayed at the Mirage previously for an extended period of time, and the desktop computer is consistent with a lengthy stay.

12. Based on the electronic evidence reviewed thus far in this investigation, the defendants communicated with each other by telephone calls, text messages and emails. In addition, they communicated with their employees or other possible co-conspirators by telephone calls, text messages and emails. They communicated with vendors of consumer debt portfolios by telephone calls and emails. They communicated with their investors and potential investors by telephone calls and emails. In addition, MERRILL, LEDFORD, and JEZIERSKI sent emails to investors or potential investors that contained fictitious and fraudulent Portfolios Sales Agreements ("PSAs"), earning statements, and bank statements as well as wire transfer instructions. Particularly, in May 2018, the FBI conducted an undercover operation in Dallas, Texas where an undercover FBI agent posed as a potential investor and met with MERRILL, LEDFORD, and JEZIERSKI. Leading up to that meeting and for some time afterward, MERRILL communicated with the undercover FBI agent through text messages and emails. Your affiant believes that copies of transmissions to investors are all contained on the seized or

18 - 3522 JMC

abandoned electronic devices A1 - A6.

18 - 3523 JMC

13. Your affiant's review of the iPhone seized from MERRILL at the time of his arrest and searched pursuant to a federal search warrant issued for MERRILL's residence at 1848 Circle Road, Towson, Maryland revealed multiple emails between MERRILL, LEDFORD, and JEZIERSKI that were sent prior to their indictment. These emails show communication both between MERRILL, LEDFORD, and JEZIERSKI and their communication with and about investors. For example, on September 17, 2018, a portfolio manager from an investment group in Dallas, Texas, known by your affiant to be a victim in this investigation, emailed MERRILL, LEDFORD, and JEZIERSKI asking to "check on the below and see what the status was on the following items in yellow that still needs to be provided." The items listed in yellow were:

- *Chrysler/Santander*
- *National Loan Exchange*
- *Garnet Capital*
- *DeVille is also going to provide the redacted RFO they received from Chase*

14. Your affiant knows that National Loan Exchange and Garnet Capital are debt brokers. National Loan Exchange, as described in the Indictment, was one of the entities MERRILL, LEDFORD, and JEZIERSKI mimicked using the acronym NLEX, to defraud money from investors. Also, Chrysler and Santander were issuers of charged off debt that MERRILL, LEDFORD, and JEZIERSKI frequently claimed to investors were sellers of debt to the MERRILL-LEDFORD-JEZIERSKI entities, when in reality the three defendants used investors' monies for personal expenditures and to pay back other investors, and used a small fraction of investors' funds to purchase debt portfolios.

15. The ongoing federal investigation has uncovered probable cause to believe that beginning in at least 2013, LEDFORD and MERRILL engaged in a scheme to defraud investors and lenders by promising to use investor/lender funds to purchase portfolios of consumer debt,

18 - 3522 JMC

18 - 3523 JMC

such as charged off credit card, car loans, or student loans, collect on the debt, or sell the portfolios, pay the investors/lenders a significant profit or interest rate, and return their principal. LEDFORD, MERRILL and JEZIERSKI, through their various companies and entities, obtained funds from investors and lenders, placed those funds into accounts that appeared to be held in the name of legitimate businesses, and then transferred the money to pay back other investors or lenders with those funds or divert the funds for their personal use. The co-conspirators furnished false documentation to the investors including inflated PSAs for the debt portfolios and bank account information for accounts which mimicked the names of legitimate debt sellers such as NLEX and SCUSA (Santander Credit USA).

16. Your affiant's investigation has revealed that LEDFORD and MERRILL failed to invest millions of dollars of investor and lender funds, that LEDFORD and MERRILL used investor or lender funds to pay other investors or lenders their principal or their purported returns, and that LEDFORD and MERRILL diverted significant amounts of investor or lender monies for personal gain to include personal credit card expenses, jewelry, cars and gambling expenses. Based on your affiant's training and experience, this pattern of conduct is indicative of a Ponzi scheme.

17. Your affiant is aware that LEDFORD and MERRILL were using multiple companies to further their fraudulent investment scheme, to include, but not limited to, DE VILLE, RIVERWALK, SCUSA FINANCIAL INC., and NLEX, INC, DELMARVA Capital, RHINO CAPITAL and GLOBAL CREDIT RECOVERY. LEDFORD and MERRILL used these companies as conduits for the funds from investors and lenders and a pattern of transfers to disguise the Ponzi nature of their scheme to defraud.

18. Your affiant's investigation has involved two email search warrants, a warrant for LEDFORD's business email account, jledford@rwfincorp.com, and one for MERRILL's email

18 - 3522 JMC

18 - 3523 JMC

account, Kevin@gcrinvest.com. Based on the actual inspection of the results of these warrants, the defendants have written and received thousands of emails to communicate with one another, with investors and prospective investors by email, with financial institutions where they have personal and entity accounts, and with sellers of debt portfolios. I am aware that computer equipment was used to generate, store, and print documents used in the fraud scheme and the money laundering conspiracy.

19. The email communications are not only messages but the transmission of attached documents such as spreadsheets which purport to show collections activity, investors' monies and portfolio purchases, and contracts with portfolios sellers and/or brokers and MERRILL and LEDFORD entities. Affiant knows that electronic devices which link to the Internet are required to create and store these records and for these emails and transmissions.

20. In addition, your affiant's investigation has revealed that LEDFORD and MERRILL both used cellular telephones which linked to the Internet and that LEDFORD used his cellular telephone while LEDFORD was in Las Vegas, Nevada. Investigators have obtained cellular telephone records for LEDFORD and MERRILL which show that the two co-conspirators were in frequent contact with each other.

21. As part of the investigation, your affiant obtained and reviewed bank accounts for entities associated with LEDFORD. A preliminary financial analysis for the period January 1, 2013 to through September 18, 2018, the date LEDFORD was arrested, indicated that LEDFORD obtained approximately \$172.7 million from lenders/investors. Approximately \$137.8 million was used to pay lenders/investors their purported profits as would be expected in a Ponzi scheme. Approximately \$31.3 million was spent on LEDFORD's personal expenses including credit cards,

18 - 3522 JMC

18 - 3523 JMC

jewelry, cars and \$24.2 million at casinos. The analysis also indicated approximately \$29.6 million was obtained from the actual collection of debt.

22. Your affiant has obtained financial records that show JEZIERSKI opened a bank account at J.P. Morgan Chase in the name of NLEX, Inc. ending in 8330. The account opening documents show that JEZIERSKI is the sole signer on the account. An initial financial analysis of NLEX, Inc. account ending in 8330 for the period January 2018 through February 2018, indicates that \$10.7 million was received from MERRILL controlled entities on January 25, 2018, sourced from investors. JEZIERSKI immediately transferred \$10.6 million to a DE VILLE account and later transferred \$150,673 on February 20, 2018 to a DE VILLE account.

23. Your affiant reviewed records for DE VILLE that showed on January 26, 2018, eight days after NLEX Inc. formation documents were filed with the State of Texas, \$30,000 was wired from DE VILLE to CRJ Holdings, LLC's J.P Morgan Chase bank account ending 5363. JEZIERSKI is the sole signer on the CRJ Holdings, LLC J.P. Morgan Chase bank account ending in 5363.

24. Your affiant believes that NLEX Inc. was created for the purpose of defrauding investors into believing that their funds were being wired to a legitimate credit portfolio broker, National Loan Exchange, when, in fact, their funds were sent to accounts controlled by JEZIERSKI, who transferred the investment funds to DE VILLE's accounts which were controlled by LEDFORD.

25. Devices A1 to A2 are currently in the lawful possession of the FBI. They came into the FBI's possession when they were turned over to the FBI by Mirage Hotel and Casino security staff after being abandoned by LEDFORD at the time of his arrest. Device A3 was seized by the FBI incident to LEDFORD's arrest. Devices A4 to A6 are also currently in the

18 - 3522 JMC 18 - 3523 JMC

lawful possession of the FBI and were seized from JEZIERSKI incident to his arrest. Therefore, while the FBI might already have all the necessary authority to examine **Devices A1 to A6**, your affiant seeks this additional warrant out of an abundance of caution to be certain that an examination of **Devices A1 to A6** will comply with the Fourth Amendment and other applicable laws.

26. **Devices A1 to A6** are currently in storage at the Evidence Control Center, FBI Baltimore Field Office, 2600 Lord Baltimore Drive, Baltimore, Maryland. In my training and experience, your affiant knows that the Devices have been stored in a manner in which is contents are, to the extent material to this investigation, in substantially ~~the same state as they~~ ~~LOGGED~~ ~~ENTERED~~ ~~RECEIVED~~ were when the Devices first came into possession of the FBI.

JAN 03 2019

TECHINCAL TERMS

27. Based on my training and experience, your affiant uses the following terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving

18 - 3522 JMC 18 - 3523 JMC

video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- b. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- d. A laptop computer is an portable electronic computing and storage device with the capability of connecting to the Internet, storing and manipulating large volumes of data, and through software programs installed on the device, performing a wide variety of functions, including the creation of documents, including spreadsheets and altered documents like the ones sent to investors in this case.

18 - 3522 JMC 18 - 3523 JMC
ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on the Target Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

18 - 3522 JMC

18 - 3523 JMC

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Target Devices were used, the purpose of the use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file. Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store

QXm'D
18 - 3522 JMC

18 - 3523 JMC

configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

18 - 3522 JMC

18 - 3523 JMC

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Target Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Target Devices to human inspection in order to determine whether it is evidence described by the warrant.

32. *Manner of execution.* Because this warrant seeks only permission to examine Target Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. Your affiant submits that this affidavit supports probable cause for a search warrant authorizing the examination of Target Devices A1 to A6 to conduct the search and seek the evidence described in Attachment B.

REQUEST FOR SEALING

34. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that the disclosure of this affidavit could

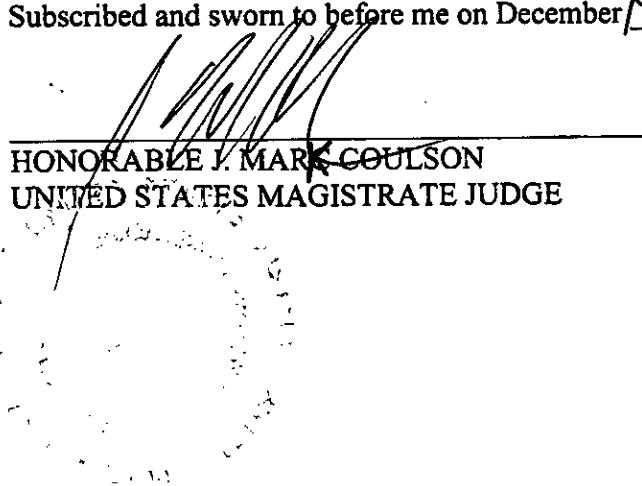
18 - 3522 JMC

18 - 3523 JMC

compromise. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation.


GEORGE J. WAHL
SPECIAL AGENT
FHFA-OIG

Subscribed and sworn to before me on December 18, 2018.


HONORABLE J. MARK COULSON
UNITED STATES MAGISTRATE JUDGE